(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－325881

(43)公開日　平成９年(1997)12月16日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　7/58			Ｇ０６Ｆ　7/58	Ａ

審査請求　有　　請求項の数５　ＯＬ　（全 ９ 頁）

(21)出願番号　特願平8－142057

(22)出願日　平成８年(1996)６月５日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　島田　道雄
東京都港区芝五丁目７番１号　日本電気株式会社内

(74)代理人　弁理士　▲柳▼川　信

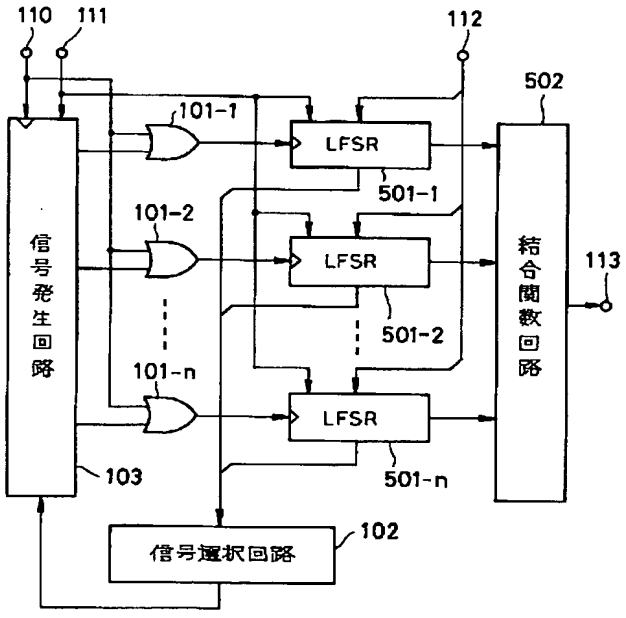
(54)【発明の名称】　擬似乱数発生装置

(57)【要約】

【課題】　複数のパルスから構成されるクロックの入力に応じて夫々シフト動作するｎ個（ｎは正の整数、以下同じ）のシフトレジスタと、このｎ個のシフトレジスタの各出力を結合して擬似乱数を生成する結合関数回路とを含む擬似乱数発生装置において、シフトレジスタの段数や個数を増加せずに、コリレーションアタックされにくいようにする。

【解決手段】　ｎ個のシフトレジスタに入力されるクロックのパルスを間引く。この場合、ｎ個のシフトレジスタに同一時刻に入力されるパルスのうちの１つのみを間引く。

【効果】　一般的に用いられている４入力の結合関数回路を使っても、非線形性の高い擬似乱数を生成できる。



1

【特許請求の範囲】

【請求項１】　複数のパルスから構成されるクロックの入力に応じて夫々シフト動作するｎ個（ｎは正の整数、以下同じ）のシフトレジスタと、このｎ個のシフトレジスタの各出力を結合して擬似乱数を生成する結合関数回路とを含む擬似乱数発生装置であって、前記ｎ個のシフトレジスタに入力されるクロックのパルスを間引くクロック間引き手段を含むことを特徴とする擬似乱数発生装置。

【請求項２】　前記クロック間引き手段は、前記ｎ個のシフトレジスタに同一時刻に入力されるパルスのうちの１つのみを間引くことを特徴とする請求項１記載の擬似乱数発生装置。

【請求項３】　前記結合関数回路はｔ次（ｔは正の整数、以下同じ）コリレーションイミューンであり、前記クロック間引き手段は長さＬ（Ｌは正の整数、以下同じ）でハミング重みがＬ×ｔ／ｎ以下の互いに異なるｎ種類の２値系列をクロックとして前記ｎ個のシフトレジスタに入力せしめ、前記シフトレジスタは入力される２値系列の値が“０”のときにシフト動作を行うことを特徴とする請求項１又は２記載の擬似乱数発生装置。

【請求項４】　前記シフトレジスタは、線形フィードバックシフトレジスタであることを特徴とする請求項１～３のいずれかに記載の擬似乱数発生装置。

【請求項５】　前記シフトレジスタは、非線形フィードバックシフトレジスタであることを特徴とする請求項１～３のいずれかに記載の擬似乱数発生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は擬似乱数発生装置に関し、特に通信システムや計算機システムにおいて採用され、許可されていない者が不正に情報を取得すること等を防止するために、情報に擬似乱数を排他的論理和で加算して暗号に変換したり暗号に擬似乱数を排他的論理和で加算して元の情報を復元するストリーム暗号装置等に用いられる擬似乱数発生装置に関する。

【０００２】

【従来の技術】従来から広く知られている暗号として、ストリーム暗号と呼ばれるものがある。これは、擬似乱数発生装置によって生成される擬似乱数系列と、送信する情報系列との排他的論理和を、暗号系列として送信するものである。なお、一般的には、情報系列が“００００・・・”であっても不正解読ができないように、ストリーム暗号が設計される。情報系列が“０００００・・・”の場合には、ストリーム暗号の出力する暗号系列から情報系列を不正解読することと、擬似乱数から擬似乱数発生装置の内部状態を推定することとは等価である。このため、以下では、「ストリーム暗号が不正解読されるという代わりに、単に「擬似乱数発生装置が不正解読される」ということもある。

2

【０００３】また、従来から広く知られている擬似乱数発生装置として、複数の線形フィードバック・シフトレジスタ（Ｌｉｎｅａｒ　Ｆｅｅｄｂａｃｋ　Ｓｈｉｆｔ　Ｒｅｇｉｓｔｅｒ；以下、ＬＦＳＲと略す）の出力する擬似乱数を、結合関数と呼ばれる非線形関数によって非線形結合して、より非線形性の高い擬似乱数を生成する方法がある。ここで、非線形結合とは線形結合ではない結合のことであり、ビットx_1，…，x_n（ｎは正の整数、以下同じ）の線形結合とは$y=x_1+x_2+\cdots x_n$や$y=x_1+x_2+\cdots x_n+1$など、排他的論理和＋だけを使ってビットｙを与えることである。言い換えると、、ビットx_1，…，x_nの非線形結合とは、$y=x_1*x_2+x_2*x_3+\cdots+x_n*x_1$等、論理積＊と排他的論理和＋との両方を使ってビットｙを与えることであり、ｙを与える式をどのように変形しても線形結合に帰着しないようなものである。また、非線形結合の非線形性とは、ｙを与える式の次数のことであり、式の次数が大きいほど非線形性が高いといわれる。なお、当然のことながら、結合関数の入力を増やせば増やすほど、非線形性の高い非線形結合が実現可能になる。

【０００４】図６は、従来の擬似乱数発生装置の構成を示すブロック図である。図において、ｎ個のＬＦＳＲ５０１－１～５０１－ｎは、入力端子５１１に“０”が供給されているときには、入力端子５１０にパスが入力されると、入力端子５１２から供給される初期状態と呼ばれるビット系列を、内部状態として保持する。なお、それぞれのＬＦＳＲ５０１－１～５０１－ｎには、一般にはＬＦＳＲ毎に異なった初期状態が供給される。また、ＬＦＳＲ５０１－１～５０１－ｎは、入力端子５１１に“１”が供給されているときには、入力端子５１０にパルスが１個入力される毎に、擬似乱数を出力する。ｎ個のＬＦＳＲ５０１－１～５０１－ｎの出力する擬似乱数は、結合関数回路５０２に入力され、結合関数回路５０２の出力が、擬似乱数として出力端子５１３から出力される。

【０００５】なお、図６の擬似乱数発生装置に、擬似乱数を発生させるには、次のようにする。まず、入力端子５１２に初期状態を供給する。次に、入力端子５１１に“０”を供給して、入力端子５１０にパルス（あるいはクロックと呼ぶ）を１個入力する。そして、入力端子５１１に“１”を供給する。すると、それ以降は、入力端子５１０にパルスを１個入力する毎に、出力端子５１３から擬似乱数が得られる。

【０００６】図７は、ＬＦＳＲ５０１－１～５０１－ｎを示す機能ブロック図である。図において、シフトレジスタ６０１は、入力端子６１１に“０”が供給されているときには、入力端子６１０にパルスが入力されると、入力端子６１２から供給される初期状態と呼ばれるビット系列を、内部状態として保持する。また、シフトレジスタ６０１は、入力端子６１１に“１”が供給されてい

るときには、入力端子６１０にパルスが１個入力されると、保持されているビット系列を右側に１ビットだけシフトして、排他的論理和回路６０２の出力をビット系列の左端のビットとして保持する。なお、ビット系列の右端に保持されていたビットは、保持されているビット系列が右側に１ビットだけシフトされると、捨てられる。

【０００７】また、シフトレジスタ６０１に保持されているビット系列は、出力端子６１３に供給されている。排他的論理和回路６０２は、シフトレジスタ６０１に保持されているビット系列のうち、予め決められた位置にあるビットの排他的論理和を計算して、計算結果をシフトレジスタ６０１に供給する。排他的論理和回路６０２の出力は、出力端子６１４にも供給されており、それが擬似乱数として出力される。ＬＦＳＲ５０１－１～５０１－ｎの構造は全て同一であるが、シフトレジスタ６０１の長さと、シフトレジスタ６０１に記憶されているビットのうち排他的論理和回路６０２に供給されるビットの位置は、一般に、ＬＦＳＲ毎に異なっている。なお、入力端子６１０，６１１，６１２には、それぞれ図６の入力端子５１０，５１１，５１２から入力される値が供給されており、出力端子６１４の出力は図６の結合関数５０２に供給されている。出力端子６１３の出力は、図６においては、使われていない。

【０００８】結合関数回路５０２とは、入力されたビットの非線形結合をとってその結果を出力する結合関数の機能を持つものであり、論理関数回路やリード・オン・メモリ（ＲＯＭ）あるいはそれらの組合わせによって表現される。図８は、４入力の結合関数回路５０２の一例を示す機能ブロック図である。これは、ｎ＝４とした擬似乱数発生装置で使われるもので、４個のＬＦＳＲ５０１－１～５０１－４の出力する擬似乱数が、それぞれ入力端子７０１－１～７０１－４に供給される。

【０００９】論理積回路７０１は、入力端子７１０－１に供給される値と入力端子７１０－２に供給される値の論理積を計算して、その結果を出力する。論理積回路７０２は、入力端子７１０－１に供給される値と入力端子７１０－３に供給される値の論理積を計算して、その結果を出力する。論理積回路７０３は、入力端子７１０－２に供給される値と入力端子７１０－３に供給される値の論理積を計算して、その結果を出力する。排他的論理和回路７０４は、論理積回路７０１の出力と論理積回路７０２の出力と論理積回路７０３の出力と入力端子７１０－４に供給される値との排他的論理和を計算し、計算結果を出力端子７１１から出力する。出力端子７１１の出力は図６の出力端子５１３に供給されている。

【００１０】しかしながら、従来の擬似乱数発生装置のＬＦＳＲ５０１－１～５０１－ｎに与えられた初期状態は、しばしば、コリレーション・アタック（ｃｏｒｒｅｌａｔｉｏｎ　ａｔｔａｃｋ）と呼ばれる解読方法で推定されてしまう。すなわち、あるＬＦＳＲ５０１－ｊ

（ｊ＝１～ｎ）の出力で条件付けたときの結合関数回路５０２の出力の条件付き確率分布が一様でない場合には、そのＬＦＳＲ５０１－ｊと等価なＬＦＳＲの出力系列と結合関数回路５０２の出力系列との相関を最大にするような等価ＬＦＳＲの初期状態を総当りで求めることで、ＬＦＳＲ５０１－ｊに与えられた初期状態が求められてしまう。

【００１１】また、一般的に、あるｔ個のＬＦＳＲの出力で条件付けたときの結合関数回路５０２の出力の条件付き確率分布が一様でない場合には、それらのｔ個のＬＦＳＲと等価なｔ個のＬＦＳＲの出力系列と結合関数回路５０２の出力系列との相関を最大にするようなｔ個の等価ＬＦＳＲの初期状態を総当りで求めることで、ｔ個のＬＦＳＲに与えられた初期状態が求められる。なお、以上の説明では、説明の便宜上、結合関数回路５０２の出力系列からＬＦＳＲの初期状態を推定することを考えたが、情報系列は理想的な乱数ではなく冗長度を持っているので、以上の操作において、結合関数回路５０２の出力系列の代わりに暗号系列を用いても、ＬＦＳＲの初期状態を推定できる。すなわち、コリレーション・アタックは、情報系列が“００００・・・”でない場合でも、実行可能である。

【００１２】なお、注意しておくが、何次までのコリレーション・アタックが実行できるか否かは、結合関数の性質だけでなく、ｔ個のＬＦＳＲの段数の合計にも依存して決まる。例えば、ｔ個のＬＦＳＲの段数の合計が６４ビットであれば、求める初期状態を総当りで求めることが困難になるので、ｔ次のコリレーション・アタックは実行できないが、ｔ個のＬＦＳＲの段数の合計が２０ビットであれば、ｔ次のコリレーション・アタックは容易に実行できる。

【００１３】このため、従来は、（ｔ＋１）次のコリレーション・アタックが実行できなくなるほどＬＦＳＲの段数を増やすと共に、ｔ個のＬＦＳＲの出力で条件付けたときの結合関数の出力の条件付き確率分布が一様であるような結合関数を用いて、ｔ次のコリレーション・アタックを防いでいた。なお、そのような結合関数は、ｔ次コリレーション・イミューン（ｃｏｒｒｅｌａｔｉｏｎ　ｉｍｍｕｎｅ）であると言われる。例えば、４入力の結合関数を用いる場合には、結合関数を１次コリレーション・イミューンにできることが知られているので、２次のコリレーション・アタックが実行できないようにＬＦＳＲの段数が選択される。なお、図６の４入力結合関数回路は、１次コリレーション・イミューンであることが知られている。

【００１４】なお、従来の擬似乱数発生装置及びコリレーション・アタックや４入力結合関数に関しては、例えば、特開平７－１０４９７６号公報や、１９８６年にスプリンガー・ヴァーラグから刊行されたルエッペル著「アナリシス・アンド・デザイン・オブ・ストリーム・

サイファー」（R. A. Rueppel著Analysis and Design of Stream Ciphers, Springer-Verlag, １９８６）の第９２頁から第１４１頁にかけてや、島田道雄著「結合関数の無相関性について」（第１７回情報理論とその応用シンポジウム予稿集１９９４年）の第５３頁から第５６頁にかけて詳しい解説がある。

【００１５】

【発明が解決しようとする課題】従来の擬似乱数発生装置の問題点は、上述した文献（島田道雄著「結合関数の無相関性について」）で示されているように、コリレーション・イミューンな結合関数を使っていても、差分コリレーション・アタックで解読できるということである。その理由は、例えば、図６の４入力結合関数回路を考えてみれば分かる。図８の４入力結合関数回路の場合には、入力端子７１０－４の入力が線形結合しているので、入力端子７１０－４に擬似乱数を供給しているＬＦＳＲの周期をＬとすると、時刻ｔと時刻Ｌ＋ｔとにおける結合関数の出力の差分をとることで、そのＬＦＳＲの出力の影響が結合関数の出力の差分に出なくなるようにすることができる。そうすると、４入力の結合関数に基づく擬似乱数発生装置を１次コリレーション・アタックで解読することが、３入力結合関数に基づく擬似乱数発生装置を１次コリレーション・アタックで解読することに帰着してしまう。３入力結合関数は、１次コリレーション・イミューンにできないので、１次コリレーション・アタックで簡単に解読されてしまう。

【００１６】本発明は上述した従来技術の欠点を解決するためになされたものであり、その目的は、ＬＦＳＲの段数や個数を増やさずに、ＬＦＳＲに供給されるクロック信号を制御することで、ストリーム暗号に適した擬似乱数発生装置を提供することである。

【００１７】

【課題を解決するための手段】本発明による擬似乱数発生装置は、複数のパルスから構成されるクロックの入力に応じて夫々シフト動作するｎ個（ｎは正の整数、以下同じ）のシフトレジスタと、このｎ個のシフトレジスタの各出力を結合して擬似乱数を生成する結合関数回路とを含む擬似乱数発生装置であって、前記ｎ個のシフトレジスタに入力されるクロックのパルスを間引くクロック間引き手段を含むことを特徴とする。

【００１８】

【発明の実施の形態】本発明の作用は以下の通りである。

【００１９】さて、良く考えてみると、コリレーション・アタックが成功するためには、次の２つの条件が必要であることが分かる。すなわち、第１の条件は、解読者が擬似乱数発生装置のＬＦＳＲと等価なＬＦＳＲを持っており、解読者が等価なＬＦＳＲの初期状態を適切に設定することで、その等価ＬＦＳＲに、擬似乱数発生装置のＬＦＳＲと同じ擬似乱数系列を発生させられるというものである。また、第２の条件は、既に述べたように、結合関数の入出力間に相関があるというものである。

【００２０】これらの２つの条件が揃わないとコリレーション・アタックが実行できないのである。そして、従来は、第２の条件を崩すことで、すなわち、結合関数の入出力間に相関が出ないようにすることで、コリレーション・アタックを防いでいたのである。

【００２１】そこで本発明では、第１の条件を崩すことで、コリレーション・アタックを防ぐことにした。すなわち、従来の擬似乱数発生装置では、それぞれのＬＦＳＲに常にクロック信号を供給していたのだが、本発明では、クロックのパルスを間引いてクロック信号のパターンを変化させることにした。すなわち、従来は、“００００・・・・”というクロック信号を使っていたのに対して、本発明では、それ以外の２値系列もクロック信号として使用することにした。クロック信号のパターンを解読者に秘密にしておけば、複製されたＬＦＳＲに擬似乱数発生装置のＬＦＳＲと同じ擬似乱数発生系列を発生させられないので、第１の条件が崩れ、コリレーション・アタックが実行できなくなる。

【００２２】なお、以上では、クロック信号を２値系列として表現したが、２値系列のτ番目が“０”であるということは、クロック信号のτ単位時刻にパルスが有ることを意味し、２値系列のτ番目が“１”であることは、クロック信号のτ単位時刻にパルスが無いことを意味する（“０”と“１”とを入れ替えても良いのだが、説明の便宜上、このようにしておく）。また、単位時刻とは、クロック信号の周期すなわちパルス１個の長さに相当する時刻を“１”として測った時間のことである。

【００２３】ただし、ただ単にランダムにクロック信号のパターンを選択するのでは、擬似乱数発生装置の出力する擬似乱数の周期が極端に短くなる危険性がある。例えば、どのＬＦＳＲも周期Ｔビットの周期系列を擬似乱数系列として出力したら、擬似乱数発生装置の出力する擬似乱数系列も周期Ｔビットの周期系列になってしまう。擬似乱数系列の周期が短いと、例えば、盗聴によって得られた擬似乱数系列全体をメモリに記憶しておき、それを暗号系列に排他的論理和で加算することで、簡単に不正解読されてしまう。

【００２４】そこで本発明では、次のような工夫によって、擬似乱数の周期が短くなることを防いでいる。すなわち、クロック信号として、互いに長さとハミング重みとが等しいｎ個の２値系列から構成されるｎ個組を、予め複数個選んでおき、それら複数個のｎ個組みからランダムに１つのｎ個組を選択し、選択されたｎ個組みの各２値系列を、ｎ個のＬＦＳＲのそれぞれに逐次的に供給する。例えば、ｎ＝４の場合には、次のようにする。

【００２５】まず、４個組みとして、（０００１，００

１０，０１００，１０００）（４単位時刻分），（１０００，０１００，００１０，０００１），（４単位時刻分）（０，０，０，０）（１単位時刻分）を用意しておく。そして、ある時刻に１番目の４個組みが選択されたならば、その４個組みの２値系列の長さは“４”であるから、次の４単位時刻までは、ＬＦＳＲ５０１－１には、“０００１”を、ＬＦＳＲ５０１－２には“００１０”を、ＬＦＳＲ５０１－３には“０１００”を、ＬＦＳＲ５０１－４には“１０００”をそれぞれクロック信号として供給する。すると、“１”の場合にクロックパルスが間引かれ、次の４単位時刻後までには、どのＬＦＳＲにも３個のパルスが供給されることになる。このことは、結果だけを見れば、どのＬＦＳＲにも“０００”というクロック信号が供給されたのと等価である。つまり、“０”の場合にはＬＦＳＲはシフト動作を行い、“１”の場合にシフト動作を行わない。また、各ＬＦＳＲに供給されるクロック信号の“１”の位置が互いに異なるので、各ＬＦＳＲに同一時刻に入力されるパルスのうちの１つのみを間引くことになる。

【００２６】以上のようにすれば、本擬似乱数発生装置のＬＦＳＲの内部状態が、少なくとも特定の時刻においては、従来の擬似乱数発生装置のＬＦＳＲの内部状態と同様に推移する。このため、擬似乱数発生装置の出力する擬似乱数系列の周期が擬似乱数発生装置の出力する擬似乱数発生系列の周期よりも短くなることはない。

【００２７】ただし、ただ単にクロック信号として、互いに長さとハミング重みとが等しい２値系列から構成されるｎ個組を用いるのでは、依然として、簡単に不正解読される危険性がある。なぜなら、前述の例において、例えば、ハミング重みが“３”である（１１１０，１１０１，１０１１，０１１１）という２値系列の４個組みを用いると、ある時刻に出力された擬似乱数と次の時刻に出力された擬似乱数との間に相関が生じることがあるからである。すなわち、４入力の結合関数は高々１次コリレーション・イミューンであり、クロック信号のハミング重みが“３”であれば、ある時刻と次の時刻とでは３個のＬＦＳＲの出力が等しくなることがあるからである。

【００２８】そこで、本発明では、結合関数がｔ次コリレーション・イミューンであれば、長さＬのクロック信号として、ハミング重みがＬｔ／ｎであるような２値系列だけを使用する。例えば、ｎ＝４の場合には、結合関数が１次コリレーション・イミューンであれば、長さ“４”のクロック信号として、ハミング重みが“１”であるような、“０００１”，“００１０”，“０１００”，“１０００”といった“１”の位置が互いに異なる２値系列だけを、ｎ個組みの要素として使用するのである。そのようにすれば、ある時刻と次の時刻とで出力が常に等しいのは１個のＬＦＳＲだけになるから、１次コリレーション・イミューンな結合関数を使うことで、ある時刻に出力された擬似乱数と次の時刻に出力された擬似乱数との間に相関が生じることを防ぐことができる。

【００２９】次に、本発明の実施例について図面を参照して詳細に説明する。

【００３０】図１は、本発明の擬似乱数発生装置の一実施例の構成を示すブロック図であり、図６と同等部分は同一符号により示されている。

【００３１】図において、本実施例の擬似乱数発生装置は、クロックが入力されるごとに１ビットの擬似乱数を生成するｎ個のＬＦＳＲ５０１－１～５０１－ｎと、これらｎ個のＬＦＳＲの出力する擬似乱数を非線形結合してビットを生成するｔ次コリレーション・イミューンな結合関数回路と、ｎ個のＬＦＳＲに記憶されたビットのうち予め決められた一部又は全部のビットに予め決められた非線形変換を施して予め決められた個数のビットを出力する信号選択回路１０２と、信号選択回路１０２の出力に依存して、長さがＬでハミング重みがＬｔ／ｎ以下であるようなｎ個の２値系列を、外部から入力されるクロックに同期して逐次に出力する信号発生回路１０３と、外部から入力されるクロックと信号発生回路１０３の出力との論理和を演算して、その演算結果をｎ個のＬＦＳＲにクロックとして供給するｎ個の論理和回路１０１－１～１０１－ｎとを含んで構成され、外部から入力されるクロックに同期して結合関数回路５０２より擬似乱数を出力する。

【００３２】ＬＦＳＲ５０１－１～５０１－ｎは、入力端子１１１に“０”が供給されているときには、論理和回路１０１－１～１０１－ｎからパルスが供給されると、入力端子１１２から供給される初期状態と呼ばれるビット系列を、内部状態として保持する。また、ＬＦＳＲ５０１－１～５０１－ｎは、入力端子１１１に“１”が供給されているときには、論理和回路１０１－１～１０１－ｎからパルスが供給されるごとに、内部状態を更新すると共に擬似乱数を出力する。そして、ＬＦＳＲ５０１－１～５０１－ｎの出力する擬似乱数が、結合関数回路５０２に入力されて、結合関数回路５０２の出力が、擬似乱数として出力端子１１３から出力される。ＬＦＳＲ５０１－１～５０１－ｎの内部状態は、信号選択回路１０２に供給されている。なお、ＬＦＳＲ５０１－１～５０１－ｎの内部状態は、図７の出力端子６１３を介して出力される。

【００３３】信号選択回路１０２については、後で詳しく述べるが、ＬＦＳＲ５０１－１～５０１－ｎの内部状態に対して予め決められた非線形変換を施して、予め決められた数のビットを発生する。信号発生回路１０３については、後で詳しく述べるが、信号選択回路１０２の出力に応じて、予め決められたクロック信号を生成して、論理和回路１０１－１～１０１－ｎに供給する。論理和回路１０１－１～１０１－ｎは、入力端子１１０か

ら供給されるパルス系列と、信号発生回路１０３から供給されるクロック信号との論理和をとることで、クロック信号に対応するパルス系列を生成して、そのパルス系列を、それぞれＬＦＳＲ５０１－１～５０１－ｎに供給する。

【００３４】なお、図１の擬似乱数発生装置に擬似乱数を発生させるには、次のようにする。まず、入力端子１１２に初期状態を供給する。次に、入力端子１１１に“０”を供給して、入力端子１１０にパルスを１個入力する。そして、入力端子１１１に“１”を供給する。すると、それ以降は、入力端子１１０にパルスを１個入力するごとに、出力端子１１３から擬似乱数が得られる。

【００３５】図２は、ｎ＝４とする図１の擬似乱数発生装置で使われる信号選択回路１０２の基本構成の一例を示す機能ブロック図である。図において、図１のＬＦＳＲ５０１－１～５０１－４の出力が、それぞれ入力端子２１０－１～２１０－４に供給されている。配線２０１は、予め決められた配線であり、入力端子２１０－１～２１０－４から供給される信号の予め決められた一部あるいは全部を、重複も許して出力する。配線２０１の出力は、ｕ個（ｕは正の整数、以下同じ）の論理積回路２０２－１～２０２－ｕの出力は配線２０３に供給される。

【００３６】配線２０３は予め決められた配線であり、論理積回路２０２－１～２０２－ｕから供給される信号の予め決められた一部あるいは全部を、重複も許して出力する。配線２０３の出力は、５個の排他的論理和回路２０４－１～２０４－５に供給され、排他的論理和回路２０４－１～２０４－５の出力は出力端子２１１から出力される。そして、出力端子２１１の出力が、図１の信号発生回路１０３に供給される。信号選択回路１０２の出力は、ＬＦＳＲ５０１－１～５０１－４の出力に依存しているので、ＬＦＳＲ５０１－１～５０１－４の全ての初期状態を知らない第三者は、信号選択回路１０２の出力を容易には推定できない。

【００３７】図３は、ｎ＝４とする図１の擬似乱数発生回路で用いられる信号発生回路１０３の基本構成の一例を示す機能ブロック図である。図において、図１の入力端子１１０から入力される信号が入力端子３２０に供給され、図１の入力端子１１１から入力される信号が入力端子３２１に供給され、図１の信号選択回路１０２の出力が入力端子３２２に供給されている。カウンタ３０７は、入力端子３２１に“０”が供給されているときには、論理和回路３０２からパルスが供給されると、カウント値をゼロにする。また、カウンタ３０７は、入力端子３２１に“１”が供給されているときには、論理和回路３０２からパルスが供給されるごとに、カウント値を“１”だけ増加し、また、保持されているカウント値を、論理和回路３０６とデコーダ３０９とに供給する。なお、カウント値が３から“１”だけ増加したときには、カウント値は“０”に戻るものとする。

【００３８】レジスタ３０８は、論理和回路３０１からパルスが供給されると、入力端子３２２に供給されている５ビットを保持し、また、保持されている５ビットのうち、左端のビットを論理和回路３０６に供給し、それ以外の４ビットを転置回路３１０に供給する。デコーダ３０９は、カウンタ３０７の出力が“ｘ”であれば、右から“ｘ”ビット目が１であるような４ビットを出力する。すなわち、デコーダ３０９は、ｘ＝“０”，“１”，“２”，“３”に対して、それぞれ“０００１”，“００１０”，“０１００”，“１０００”を出力する。転置回路３１０は、レジスタ３０８の出力に応じて、デコーダ３０９の出力ビットの転置（すなわち位置を入れ替えたもの）を出力する。なお、どういった転置を行うかは、予め決められているものとする。

【００３９】セレクタ３１１は、論理積回路３０４の出力が“０”であれば、転置回路３１０の出力を選択して出力し、論理積回路３０４の出力が“１”であれば、“００００”を出力する。そして、セレクタ３１１の出力が出力端子３２３から出力される。なお、出力端子３２３の出力は、図１の論理和回路１０１－１～１０１－５に供給される。

【００４０】論理和回路３０６は、カウンタ３０７の出力とレジスタ３０８の出力の左端ビットとの計３ビットの論理和を計算して、その結果を出力する。否定回路３０５は、論理和回路３０６の出力を反転して、その結果を出力する。論理積回路３０３は、入力端子３２１から供給される信号と論理和回路３０６の出力の論理積を計算して、その結果を出力する。論理積回路３０４は、入力端子３２１から供給される信号と否定回路３０５の出力との論理積を計算して、その結果を出力する。論理和回路３０１は、入力端子３２０から供給される信号と論理積回路３０３の出力との論理和を計算して、その結果を出力する。論理和回路３０２は、入力端子３２０から供給される信号と論理積回路３０４の出力との論理和を計算して、その結果を出力する。

【００４１】同図の信号発生回路の動作を説明すると、次のようになる。入力端子３２１に“０”が供給されているときに、入力端子３２０にパルスが供給されると、カウンタ３０７のカウント値が“０”に設定されると共に、入力端子３２２に供給されている５ビットがレジスタ３０８に保持される。そして、入力端子３２１に“１”が供給されており、かつ、カウンタ３０７のカウント値が“０”であり、かつ、レジスタ３０８に保持されている５ビットの左端のビットが“０”であれば、セレクタ３１１から“００００”が出力され、入力端子３２０にパルスが１個入力されると、レジスタ３０８には入力端子３２２から供給される新しい５ビットが保持される。一方、入力端子３２１に“１”が供給されており、かつ、カウンタ３０７のカウント値が“０”であ

り、かつ、レジスタ３０８に保持されている５ビットの左端のビットが“１”であれば、次の４単位時刻後にカウンタ３０７のカウント値が再び“０”になるまで、出力端子３２３からハミング重みが“１”であるような４ビットが出力される。

【００４２】図４は、ｎ＝４とする図３の信号発生回路１０３で用いられる転置回路３１０の基本構成の一例を示す機能ブロック図である。図において、入力端子４１０－１～４１０－４には、図３のデコーダ３０９の出力が供給され、入力端子４１１には、図３のレジスタ３０８の出力の右４ビットが供給されている。入力端子４１０－１～４１０－４に供給された信号は、配線４０１－１に入力される。配線４０１－ｊ（ｊ＝１，２，３，４）は、４ビットの入力に対して予め決められた２通りの配線によって、予め決められた互いに異なる２通りの転置を施す。そして、夫々の転置結果を図中の左側と右側とに出力し、夫々セレクタ４０２－ｊの左側と右側とに供給する。

【００４３】セレクタ４０２－ｊ（ｊ＝１，２，３，４）には、入力端子４１１に供給されている４ビットのうち１ビットが供給されており、そのビットの値に応じて、左側あるいは右側の入力を選択して出力する。そして、セレクタ４０２－ｊ（ｊ＝１，２，３）の出力は、配線４０１－（ｊ＋１）に入力され、セレクタ４０２－４の出力は、出力端子４１２－１～４１２－４から出力される。なお、出力端子４１２－１～４１２－４から出力された４ビットは、図３のセレクタ３１１の左側の入力に供給される。

【００４４】ところで、図１中の線形フィードバックシフトレジスタ５０１－１～５０１－ｎに代えて、非線形フィードバックシフトレジスタを用いても良い。図５は、非線形フィードバックシフトレジスタの一構成例を示すブロック図である。図において、シフトレジスタ８０１は、図７のＬＦＳＲ５０１と同様の構造を持つものである。図中のシフトレジスタ８０１は、入力端子８１１に“０”が供給されているときに、入力端子８１０にパルスが入力されると、入力端子８１２から供給される初期状態と呼ばれるビット系列を、内部状態として保持する。また、シフトレジスタ８０１は、入力端子８１１に“１”が供給されているときに、入力端子８１０にパルスが１個入力されると、保持されているビット系列を右側に１ビットだけシフトして、排他的論理和回路８０２の出力をビット系列の左端のビットとして保持する。なお、ビット系列の右端に保持されていたビットは、保持されているビット系列が右側に１ビットだけシフトされると、捨てられる。

【００４５】また、シフトレジスタ８０１に保持されているビット系列は、出力端子８１３と非線形関数回路８０３に供給されている。排他的論理和回路８０２は、シフトレジスタ８０１に保持されているビット系列のうち、予め決められた位置にあるビットの排他的論理和を計算して、計算結果をシフトレジスタ８０１に供給する。非線形関数回路８０３は、シフトレジスタ８０１に保持されているビット系列のうち、予め決められた位置にあるビットの非線形結合を計算する。すなわち、予め決められた位置にあるビットに対して、予め決められた排他的論理和以外の論理演算を施す。そして、その計算結果が擬似乱数として出力端子８１４から出力される。

【００４６】要するに、線形フィードバックシフトレジスタの代わりに、非線形フィードバックレジスタを用いて擬似乱数発生装置を構成した場合でもクロックパルスを間引くことによってシフトレジスタの段数や個数を増やさずに、ストリーム暗号化に適した擬似乱数を発生することができるのである。

【００４７】以上のように、本装置を用いて擬似乱数を発生させれば、全てのＬＦＳＲの初期状態を知らない第三者には、ＬＦＳＲの内部状態がどのようなタイミングで推移しているか推測できないので、一般的に用いられている４入力の結合関数回路を使っていても、コリレーション・アタック及び差分コリレーション・アタックに強い擬似乱数を発生できるのである。これにより、比較的簡単な構成でありながら、ストリーム暗号に適した擬似乱数発生装置が実現できる。

【００４８】また、本装置では、結合関数回路において非線形な変換が行われるだけでなく、信号選択回路においても非線形な変換が行われ、その変換結果にも依存して擬似乱数が生成されるので、一般的に用いられている４入力の結合関数回路を使っていても、非線形性の高い擬似乱数を生成できるのである。これにより、ストリーム暗号に適した擬似乱数発生装置が実現できる。

【００４９】要するに本装置では、複数のパルスから構成されるクロックの入力に応じて夫々シフト動作するｎ個のシフトレジスタと、このｎ個のシフトレジスタの各出力を結合して擬似乱数を生成する結合関数回路とを含み、ｎ個のシフトレジスタに入力されるクロックのパルスを間引いているのである。これにより、比較的簡単な構成でありながら、ストリーム暗号に適した擬似乱数を発生することができるのである。

【００５０】

【発明の効果】以上説明したように本発明は、擬似乱数を発生する線形（非線形）フィードバックシフトレジスタへの入力クロックを間引くことにより、そのレジスタの初期状態を知らない第三者にはシフトレジスタの内部状態がどのようなタイミングで推移しているのか推測できず、比較的簡単な回路構成でコリレーション・アタックに強い擬似乱数を発生することができるという効果がある。

【図面の簡単な説明】

【図１】本発明の実施例による擬似乱数発生装置の構成を示すブロック図である。

13　　14

【図２】図１中の信号選択回路の内部構成例を示すブロック図である。

【図３】図１中の信号発生回路の内部構成例を示すブロック図である。

【図４】図３中の転置回路の内部構成例を示すブロック図である。

【図５】図１中のＬＦＳＲの代わりに用いる非線形フィードバックレジスタの内部構成例を示すブロック図である。

【図６】従来の擬似乱数発生装置の構成を示すブロック図である。

【図７】図６中のＬＦＳＲの内部構成例を示すブロック図である。

【図８】図６中の結合関数回路の内部構成例を示すブロック図である。

【符号の説明】

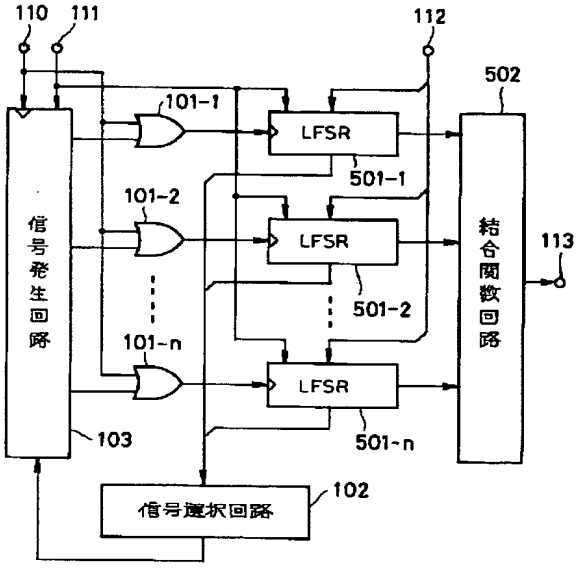
１０２　信号選択回路

１０３　信号発生回路

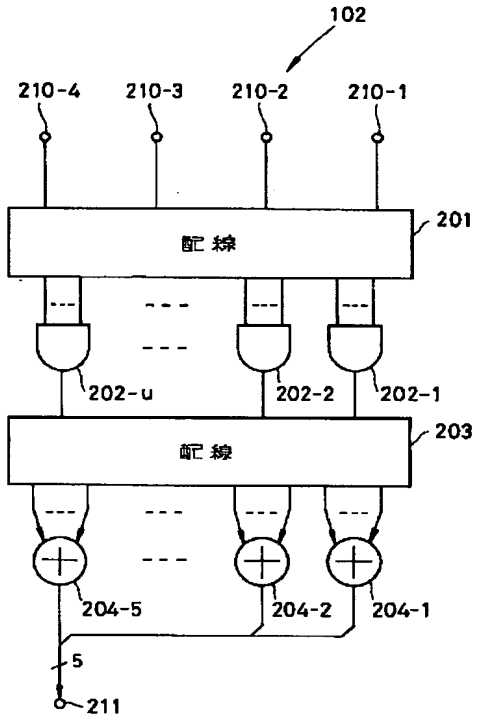
５０１－１～５０１－ｎ　ＬＦＳＲ

５０２　結合関数回路

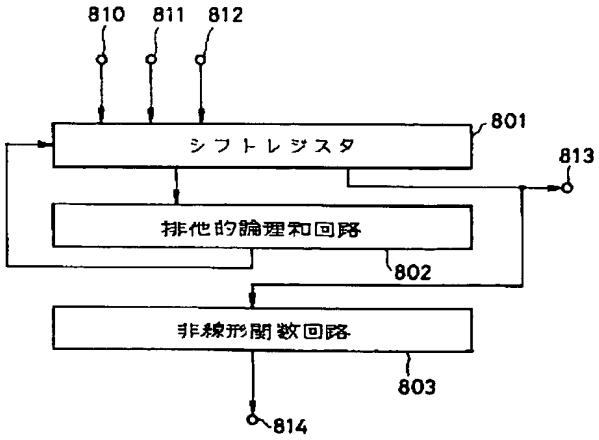
【図１】



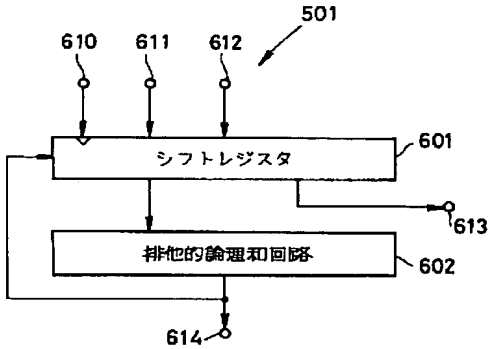
【図２】



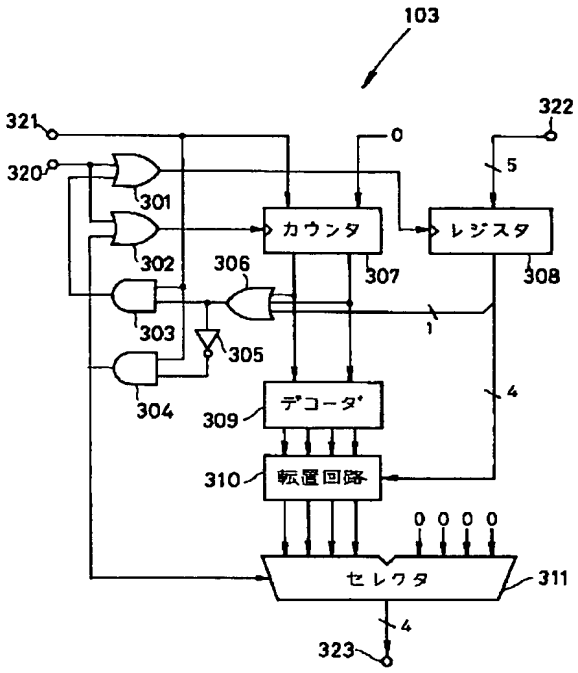
【図５】



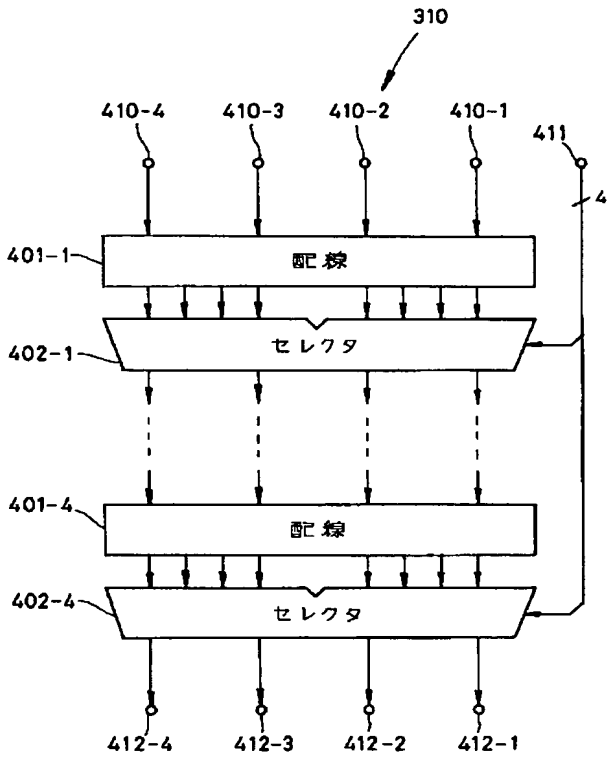
【図７】



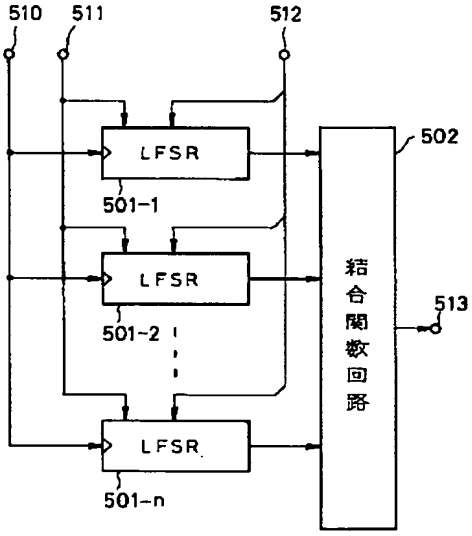
【図３】


103
321
320
322
0
5
301
302
カウンタ
レジスタ
306
307
308
303
305
1
304
309
デコーダ
4
310
転置回路
0 0 0 0
セレクタ
311
4
323

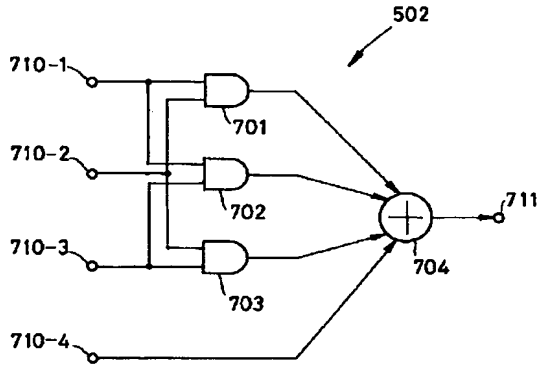
【図４】


310
410-4
410-3
410-2
410-1
411
4
401-1
配線
402-1
セレクタ
401-4
配線
402-4
セレクタ
412-4
412-3
412-2
412-1

【図６】


510
511
512
LFSR
501-1
LFSR
501-2
LFSR
501-n
502
結合関数回路
513

【図８】


502
710-1
701
710-2
702
711
710-3
703
704
710-4